
**UNITED STATES DISTRICT COURT
DISTRICT OF NEW JERSEY**

UNITED STATES OF AMERICA

v.

LARRY PATTERSON
a/k/a "Ag3nt47"

:
: Hon. James B. Clark, III
:
: Mag. No. 13-3094
:
: CRIMINAL COMPLAINT
:
:
:

I, Russell A. Ficara, being duly sworn, state the following is true and correct to the best of my knowledge and belief:

SEE ATTACHMENT A

I further state that I am a Special Agent with the Federal Bureau of Investigation, and that this complaint is based on the following facts:

SEE ATTACHMENT B

continued on the attached pages and made a part hereof.




Russell A. Ficara, Special Agent
Federal Bureau of Investigation

Sworn to before me, and
subscribed in my presence

November 22, 2013 at
Newark, New Jersey

HONORABLE JAMES B. CLARK, III
UNITED STATES MAGISTRATE JUDGE


Signature of Judicial Officer

ATTACHMENT A

Count One
(Unauthorized Computer Access)

On or about July 23, 2013, in the District of New Jersey and elsewhere, defendant

LARRY PATTERSON
a/k/a "Ag3nt47"

knowingly and intentionally accessed a protected computer without authorization, and as a result of such conduct, recklessly caused damage to University-1, which during a one-year period caused loss to one or more persons, from this conduct and the defendant's related courses of conduct, aggregating at least \$5,000 in value.

In violation of Title 18, United States Code, Sections 1030(a)(5)(B) and (c)(4)(A)(i)(I).

ATTACHMENT B

I, Russell A. Ficara, a Special Agent with the Federal Bureau of Investigation ("FBI"), having conducted an investigation and discussed this matter with other law enforcement officers who have participated in this investigation, have knowledge of the following facts. Because this Complaint is being submitted for the limited purpose of establishing probable cause, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts which I believe are necessary to establish probable cause. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance and in part.

Overview

1. The FBI has been investigating an individual using the alias "Ag3nt47," who has claimed credit for hacking into the computer networks of dozens of companies, universities and government agencies (collectively, the "Victim Entities") between in or about April 2013 and in or about August 2013. As explained below, there is probable cause to believe that defendant LARRY PATTERSON is "Ag3nt47" and is responsible for the intrusions into the computer networks of the Victim Entities.

2. At all times relevant to this Complaint:

- a. Defendant PATTERSON resided in California.
- b. Defendant PATTERSON used different methods to access the computer networks of the Victim Entities without authorization. In some instances he used "SQL injection" attacks which take aim at specific vulnerabilities in publicly-facing websites. In other instances, he used "cross-site scripting vulnerabilities" which can allow an attacker to bypass access controls and gain access to the data handled by a website.
- c. Defendant PATTERSON maintained a Twitter Account with the username Ag3nt47 (the "Ag3nt47 Twitter Account"). Records from Twitter and Comcast, an internet service provider, revealed that many of the logins to the Ag3nt47 Twitter Account originated from the home of defendant PATTERSON.
- d. On the Ag3nt47 Twitter Account, defendant PATTERSON posted claims of responsibility for hacking or attempting to hack into the computer networks of the Victim Entities. These claims frequently included screen captures illustrating his unauthorized access into the computer networks of the Victim Entities.

The University-1 Hack

3. On or about July 23, 2013, defendant PATTERSON posted a tweet on the Ag3nt47 Twitter Account and a screen capture showing the results of a SQL injection attack against University-1.

4. Records from University-1 indicate that on or about July 23, 2013, its computer network was accessed without authorization and that a SQL injection attack was launched against it. According to records from University-1, the attacker gained access to a non-public database on computers located in New Jersey.

5. Records from University-1 also indicate that at approximately the same date and time that this attack occurred, University-1's computer network was accessed from a particular IP Address owned by Comcast. Records from Comcast indicate that this IP Address was registered to the residence of defendant PATTERSON on the date of the attack on University-1.

Defendant PATTERSON's Admissions To Law Enforcement

6. On or about November 21, 2013, federal law enforcement executed a search warrant at defendant PATTERSON's home located in Tracy, California. During the execution of the search warrant, defendant PATTERSON spoke with law enforcement officers and admitted, in substance and in part, that he controlled the Ag3nt47 Twitter Account, that he was responsible for the SQL injection attack on University-1 on or about July 23, 2013, and that he was responsible for the hacks of over 30 Victim Entities.